EXHIBIT B

CV 12 – 2672

SUMMONS ISSUED

GARAUFIS, J.

ORENSTEIN, M.J.

REESE RICHMAN LLP
Kim E. Richman
krichman@reeserichman.com
Michael R. Reese
mreese@reeserichman.com
875 Avenue of the Americas, 18th Floor
New York, New York 10001
Telephone: (212) 643-0500
Facsimile: (212) 253-4272

- and -

MILBERG LLP
Sanford P. Dumain
sdumain@milberg.com
Peter E. Seidman
pseidman@milberg.com
One Penn Plaza
New York, New York 10119
Telephone: (212) 594-5300
Facsimile: (212) 868-1229

Attorneys for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF NEW YORK

DANIEL MAZZONE and MICHELLE KUSWANTO, on behalf of themselves and all others similarly situated, Plaintiffs, vs. VIBRANT MEDIA INC., Defendant.	Case No. ____________ **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Daniel Mazzone and Michelle Kuswanto (collectively, "Plaintiffs") allege the following, based upon personal knowledge and upon information and belief derived from, among other things, investigation of counsel and review of public documents.

NATURE OF THE ACTION

1. This is a class action against Vibrant Media Inc. ("Vibrant" or "Defendant") arising from Defendant's hacking of computers and mobile devices and Defendant's invasion of Internet users' online privacy.

2. Defendant circumvented the privacy protections on Plaintiffs' Safari[1] web browsers, thereby hacking into Plaintiffs' computers and mobile devices (collectively, "Devices"). Subsequently, Defendant placed cookies on Plaintiffs' Safari browsers that Defendant used to obtain information about Plaintiffs and their Devices as they used Safari to browse web pages to which Defendant delivered web content as a third party. Included in the private information that Defendant obtained in this manner was sensitive, personal, and personally identifiable information, and, as set forth herein, Defendant, without Plaintiffs' knowledge, misappropriated and exploited this private information for its own uses.

3. These actions of Defendant violated New York General Business Law § 349; California Penal Code § 502; Article I, Section 1, of the California Constitution; and California Penal Code § 630 *et seq*. Defendant's conduct also constitutes trespass to personal property / chattels under New York common law and invasion of privacy under California common law.

JURISDICTION AND VENUE

4. This Court has original jurisdiction over this class action under 28 U.S.C. § 1332(d), which, under the provisions of the Class Action Fairness Act ("CAFA"), explicitly provides for the original jurisdiction of the Federal Courts in any class action in which at least 100 members are in the proposed plaintiff class, any member of the plaintiff class is a citizen of a State different from any defendant, and the matter in controversy exceeds the sum of $5,000,000,

[1] All references to "Safari" are to the Safari web browser developed by Apple Inc.

exclusive of interest and costs. Plaintiffs allege that the total claims of individual members of the proposed Class are well in excess of $5,000,000 in the aggregate, exclusive of interest and costs.

5. Venue for this action properly lies in this District pursuant to 28 U.S.C. § 1391. Substantial acts in furtherance of the alleged improper conduct, including hacking of Plaintiffs' and the Class members' Devices, occurred within this District.

THE PARTIES

6. Plaintiff Daniel Mazzone resides in New York and uses his Devices there. Mr. Mazzone values his online privacy, especially when using the Internet in the seclusion of his home and/or when conducting his personal affairs. Mr. Mazzone browses the Internet using the Safari browser on both his iPad and computer. At all relevant times, Safari's "Third-Party-Blocking Only Option" (described in detail below) was either operating by default or had been selected by Mr. Mazzone. Mr. Mazzone used Safari to visit web pages that included advertisements (the "Hacking Ads", described in detail below) that Defendant used to hack into his Devices and, subsequently, to place tracking mechanisms called "cookies" on the Devices. Defendant used the cookies so placed, each of which was called "VM_USR", to obtain "End User Information" (as defined below) about Mr. Mazzone and his Devices as he used Safari to browse web pages to which Defendant delivered web content. In this manner, Defendant obtained private information about Mr. Mazzone and his Devices without his permission and against his will (as expressed by means of Safari's Third-Party-Blocking Only Option). Mr. Mazzone mistakenly believed that Safari's privacy controls protected him from having his information obtained by Defendant (in the manner described herein), and Mr. Mazzone mistakenly believed that Defendant's Hacking Ads were a benign part of the online environment. When Mr. Mazzone discovered that Defendant had hacked his Devices and learned and collected private information about him without his permission, Mr. Mazzone was shocked, humiliated, and angered and he suffered emotional distress. Furthermore, Defendant's conduct undermined Mr. Mazzone's faith and confidence in the trustworthiness and integrity of the Internet.

Defendant degraded the value of Mr. Mazzone's Devices and deprived him of the ability to sell to Defendant the information that Defendant collected against his will.

7. Plaintiff Michelle Kuswanto resides in California and uses her Devices there. Ms. Kuswanto values her online privacy, especially when using the Internet in the seclusion of her home and/or when conducting her personal affairs. Ms. Kuswanto browses the Internet using the Safari browser on both her iPhone and computer. At all relevant times, Safari's Third-Party-Blocking Only Option was either operating by default or had been selected by Ms. Kuswanto. Ms. Kuswanto used Safari to visit web pages that included Hacking Ads that Defendant used to hack into her Devices and, subsequently, to place the "VM_USR" cookie on the Devices. Defendant used the cookies so placed to obtain End User Information about Ms. Kuswanto and her Devices as she used Safari to browse web pages to which Defendant delivered web content. In this manner, Defendant obtained private information about Ms. Kuswanto and her Devices without her permission and against her will (as expressed by means of Safari's Third-Party-Blocking Only Option). Ms. Kuswanto mistakenly believed that Safari's privacy controls protected her from having her information obtained by Defendant (in the manner described herein), and Ms. Kuswanto mistakenly believed that Defendant's Hacking Ads were a benign part of the online environment. When Ms. Kuswanto discovered that Defendant had hacked her Devices and learned and collected private information about her without her permission, Ms. Kuswanto was shocked, humiliated, and angered and she suffered emotional distress. Furthermore, Defendant's conduct undermined Ms. Kuswanto's faith and confidence in the trustworthiness and integrity of the Internet. Defendant degraded the value of Ms. Kuswanto's Devices and deprived her of the ability to sell to Defendant the information that Defendant collected against her will. (Exhibit 1 hereto shows the results of a diagnostic test performed on Ms. Kuswanto's iPhone through the website of the Network Advertising Initiative, a self-regulatory organization comprised of over 80 online advertising companies, including Vibrant.)

8. Defendant Vibrant Media Inc. is a Delaware corporation that maintains its headquarters in New York, New York. Vibrant conducts business throughout New York, the nation, and internationally.

STATEMENT OF THE CASE

9. People have incorporated the web into their personal lives, through the use of things like social media, dating sites, digital commerce, political forums, and sites containing medical information. *See* The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 2012) (Foreword), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

10. Plaintiffs at all relevant times used the Internet to communicate with others via social media, to engage in commerce, and to search for a wide variety of information, much of it personal, sensitive, and private. They often browsed the Internet from the seclusion of their homes and at all relevant times did not expect, nor did they have any reason to expect, that outsiders would observe or record their online activities.

11. This expectation derived, in part, from various mechanisms that are designed to grant Plaintiffs control over who may access information about them and their Devices as they browse the Internet.[2] These mechanisms include the privacy controls incorporated into Apple Inc.'s Safari web browser (the "Privacy Controls").[3] Safari's Privacy Controls are adjustable at the discretion of the Safari user. At all relevant times, Plaintiffs had available a choice:

(a) They could keep their "End User Information" (as defined below) secret from all websites.

[2] The "Do Not Track" system, which allows consumers to signal to online companies that they do not want to be tracked, is one such mechanism. *See* Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* i, iii, v (Mar. 2012), *available at* http://ftc.gov/os/2012/03/120326privacyreport.pdf.

[3] The Privacy Controls only protect Internet users when they are browsing using Safari. The Privacy Controls have no effect on and cannot protect browsing conducted using other web browsers, such as Windows Internet Explorer (developed by Microsoft Corporation) or Mozilla Firefox (developed by Mozilla Foundation and Mozilla Corporation).

(b) They could keep their End User Information secret from all websites except for the websites whose web pages they visited (the "First Party Content Providers"). For example, if a Safari user chose this option and then visited a web page on the site located at http://www.amazon.com/ ("amazon.com"), Safari would allow amazon.com to set cookies on the Safari user's Device.[4] If amazon.com then set a cookie(s) on the user's Device, amazon.com could use the cookie(s), among other things, to facilitate collection of End User Information about the Safari user whenever the user visited web pages that included content provided by amazon.com, [5] to streamline the purchase process, or to facilitate recommendation of products based on the user's amazon.com browsing and purchase history. Many Internet users are willing to allow First Party Content Providers to set cookies (and thereby potentially to obtain End User Information about them) because many web pages cannot function properly (or in some cases, at all) if the First Party Content Provider cannot set cookies. This option is the default option in Safari's Privacy Controls – *i.e.*, it is the one that is operational by default and remains in operation unless the Safari user switches to another option. Herein, this option is referred to as the "Third-Party-Blocking Only Option."

(c) They could allow not only First Party Content Providers but also "Third Party Content Providers" to set cookies on their Devices and thereby potentially obtain End User Information about them as they browse the web using Safari. A "Third Party Content Provider" is a website that

[4] In this instance, amazon.com is the website acting as the First Party Content Provider.

[5] Practically speaking, a website cannot efficiently and reliably collect End User Information about an Internet user without setting a cookie on the Internet user's Device.

Case 1:12-cv-02672-NGG-JO Document 1 Filed 05/25/12 Page 9 of 30 PageID #: 7

delivers content to a web page that is part of a separate, different website, as an Internet user is visiting the page.[6] For example, when an Internet user is visiting a web page on the site located at http://www.facebook.com/ ("facebook.com"), the web page may include content (for example, an ad) delivered from the site located at http://www.third-party-advertiser.com/ ("third-party-advertiser.com"). In this instance, facebook.com is acting as a First Party Content Provider and third-party-advertiser.com is acting as a Third Party Content Provider. Herein, the content delivered by a Third Party Content Provider to a First Party Content Provider's web page is called "Third Party Content."[7]

12. A Safari user who has selected the Third-Party-Blocking Only Option can stop the Privacy Controls from keeping End User Information secret from a specific Third Party Content Provider by submitting an online form to that Third Party Content Provider (the "Form Exception").

13. As used herein, the term "End User Information" means information that a website can obtain about an Internet user after the site has set a cookie on the user's Device. The information may be obtained when the user visits either (i) a web page that is part of the site or (ii) a web page to which the site is delivering Third Party Content. End User Information includes but is not limited to the Uniform Resource Locator ("URL") of the page that the user visited (i) on the site or (ii) to which the site delivered Third Party Content; the time at which the user visited the page; details about the operating system on which the user's browser was running (for example, "Mac OS X" on an iPad); and details about the user's web browser (including information about extensions added to the browser). If a site sets a cookie on an

[6] The latter website is thus acting as a First Party Content Provider.

[7] Examples of Third Party Content include advertisements and "web beacons" (further explained herein).

Internet user's Device and the user subsequently visits a series of web pages that (i) are part of the site or (ii) are pages to which the site delivers Third Party Content, then the site can collect a list or a history of information about the user (including the information listed in this paragraph).

14. A website can thus collect End User Information about an Internet user when it provides Third Party Content to other sites throughout the web that the user visits, so long as the website has set a cookie on the user's Device. As noted in footnote 7, *supra*, Third Party Content includes but is not limited to ads and "web beacons." "Web beacons" are pieces of web content that are invisible (or extremely small).[8] When a website delivers a web beacon to a web page as Third Party Content, the Internet user visiting the page is almost always unaware that the web beacon is included on the page (unlike the case where an ad is delivered to a web page as Third Party Content). The purpose, however, of delivering a web beacon as Third Party Content to a web page is not for the Internet user visiting the page to see the web beacon. It is instead to allow the site delivering the web beacon to obtain End User Information about the user (which is, practically speaking, only possible when the Third Party Content Provider has set a cookie on the user's Device).

15. Few Internet users are willing to allow websites they have never directly visited to obtain End User Information about them, even if those sites have delivered Third Party Content to (first party) web pages that the users have visited.

16. Defendant's business includes delivering ads as Third Party Content to web pages throughout the World Wide Web on behalf of Defendant's advertiser clients.

17. Defendant's business also includes obtaining End User Information about Internet users as the users browse sites to which Defendant delivers Third Party Content (including ads

[8] Web beacons are alternatively known as "web bugs", "tags", "tracking pixels", "1 x 1 gifs", and "clear gifs". Vibrant's privacy statement explains that it uses web beacons in conjunction with cookies. *See* http://www.vibrantmedia.com/privacy.asp ("You may encounter our technology: … when one of our Clients places one of our web beacons on its website, which you visit. ***** Our Technology uses cookies in conjunction with Web beacons in order to help make the online advertisements you see more relevant to you.")

and web beacons), which is possible when Defendant has set cookies on the Internet users' Devices.

18. Defendant used computer programming language contained in some of the ads it delivered to web pages as Third Party Content (the "Hacking Ads") to disable the protection provided by Safari's Privacy Controls – the Safari users' express preference with regard to setting of cookies on their Devices, including cookies used to obtain End User Information – with respect to Defendant. *See infra* ¶ 11.

19. Specifically, when Defendant delivered a Hacking Ad as Third Party Content to a web page that was loading in a Plaintiff's or Class member's Safari browser, the computer programming language within the Hacking Ad caused the browser to *immediately* send an *invisible* online form back to Defendant, triggering Safari's Form Exception with respect to Defendant (*i.e.*, turning off Safari's privacy protections with respect to Defendant).

20. However, a Safari user is the only appropriate person to fill out and send this type of online form from the user's Device to Defendant, especially when doing so has the effect of disabling Safari's privacy protections with respect to Defendant. Defendant thus hacked Plaintiffs' and the Class members' Devices by means of the Hacking Ads.

21. After Defendant had hacked Plaintiffs' and the Class members' Devices, Safari's Privacy Controls no longer prevented Defendant from setting cookies on Plaintiffs and the Class members Devices, including cookies that Defendant could use in conjunction with Third Party Content (as described above) to obtain End User Information about Plaintiffs and the Class members.

22. Specifically, once Defendant had triggered Safari's Form Exception, Defendant was able to and did place the "VM_USR" cookie on the Device that was hacked. Each "VM_USR" cookie contains an ID that Vibrant uses for tracking purposes.

23. Stanford researcher Jonathan Mayer first identified Defendant's Hacking Ads. Mr. Mayer's blog describes these findings in detail. *See* http://webpolicy.org/2012/02/17/safari-trackers/. Subsequently, Ashkan Soltani, technology adviser for *The Wall Street Journal*,

independently confirmed Mr. Mayer's findings. Mr. Soltani surveyed the top 100 most popular websites as ranked by Quantcast in February 2012.

24. On February 17, 2012, *The Wall Street Journal* published an article describing Mr. Mayer's and Mr. Soltani's findings in detail. *See* Julia Angwin & Jennifer Valentino-Devries, *Google's iPhone Tracking: Web Giant, Others Bypassed Apple Browser Settings for Guarding Privacy*, Wall St. J., Feb. 17, 2012, *available at* http://online.wsj.com/article/SB10001424052970204880404577225380456599176.html.

25. According to *The Wall Street Journal*, Vibrant has admitted to using Hacking Ads to enable placement of ID cookies that enable it to obtain End User Information about Safari users. *The Wall Street Journal* states:

> A Vibrant Media spokesman called its use of the [Privacy Controls circumvention] technique a "workaround" to "make Safari work like all the other browsers." Other major Web browsers don't block tracking by default. Vibrant, a top 25 ad network in the U.S. according to comScore Media Metrix, uses the technique "for unique user identification," the spokesman said, but doesn't collect personally identifiable information such as name or financial-account numbers.

Angwin & Valentino-Devries, *Google's iPhone Tracking: Web Giant, Others Bypassed Apple Browser Settings for Guarding Privacy*.

26. Mr. Mayer discovered Defendant's Hacking Ads on the following sites:
http://answers.com/
http://cbslocal.com/ [various region-specific subdomains]

27. At all relevant times, Plaintiffs were unaware that Defendant had improperly disabled their Safari privacy protections to allow Defendant to collect and exploit End User Information about them, including their private Internet browsing history.

28. To prevent this, Plaintiffs and the Class members could have deleted the "VM_USR" cookie or visited certain websites and opted out of tracking by Defendant. Plaintiffs and the Class members, however, did not know that the "VM_USR" cookie was on their Devices or that Defendant was obtaining End User Information about them as they surfed the web. Plaintiffs and the Class members instead believed that Safari's Privacy Controls, which were set to the Third-Party-Blocking Only Option, prevented Third Party Content Providers (including

Defendant when it was acting as a Third Party Content Provider) from placing cookies on their Devices and obtaining End User Information about them. Plaintiffs and the Class members therefore had no reason to locate and delete the "VM_USR" cookie or to attempt to discover which websites they could use to opt out of tracking by Defendant.

29. Defendant injured Plaintiffs and the Class members by hacking their Devices.

30. As a result of being hacked, the Devices no longer functioned as they normally should have.

31. By hacking the Devices and impairing their functionality, Defendant degraded their value.

32. Upon discovering that Defendant had hacked their Devices and obtained private End User Information about them without their permission and against their will (as expressed by means of Safari's Third-Party-Blocking Only Option), Plaintiffs and the Class members were shocked, humiliated, and angered, and suffered emotional distress.

33. By the above actions, Defendant undermined Plaintiffs' and the Class members' confidence in the safety and trustworthiness of the digital environment.

The Value of People's Personal Information

34. The personal information that Defendant collected is an asset that is priced, bought, and sold in discrete units for marketing and other purposes. "Websites and stores can . . . easily buy and sell information on valued visitors with the intention of merging behavioral with demographic and geographic data in ways that will create social categories that advertisers covet and target with ads tailored to them or people like them." Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley, & Michael Hennessy, *Americans Reject Tailored Advertising and Three Activities that Enable It* (Sept. 29, 2009), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214. The more information that is known about a consumer, the more a company will pay to deliver a precisely targeted advertisement to him or her. *See* Federal Trade Commission (FTC), Protecting Consumer Privacy in an Era of Rapid Change, Preliminary Staff Report (Dec. 2010) ("FTC Report"), at 24.

35. Personal data is viewed as currency. "In many instances, consumers pay for free content and services by disclosing their personal information," according to former FTC commissioner Pamela Jones Harbour. FTC Roundtable Series 1 on: Exploring Privacy (Matter No. P095416) (Dec. 7, 2009), at 148, *available at* http://www.ftc.gov/bcp/workshops/privacyroundtables/ PrivacyRoundtable_Dec 2009_Transcript.pdf. In *Property, Privacy, and Personal Data*, Professor Paul M. Schwartz wrote:

> Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from this trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.

Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055, 2056-57 (2004).

36. On February 28, 2011, *The Wall Street Journal* highlighted a company called "Allow Ltd.," which is one of nearly a dozen companies that offers to sell people's personal information on their behalf and which gives its users 70% of such sales. *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, Wall St. J., Feb. 28, 2011, *available at* http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html. For example, one Allow Ltd. user received a payment of $8.95 for letting Allow tell a credit card company the user was shopping for a new credit card. *Id.*

37. On February 15, 2012, *The Financial Times* acknowledged the value of personal information in the Internet age in the context of Facebook, Inc.'s upcoming initial public offering: "Two weeks ago Facebook announced an initial public offering that could value the company at up to $100bn. Facebook is worth so much because of the data it holds on its 845m users."[9]

[9] Richard Falkenrath, *Google Must Remember Our Right to be Forgotten*, Fin. Times, *available at* http://www.ft.com/intl/cms/s/0/476b9a08-572a-11e1-869b-00144feabdc0.html#axzz1mgPiI5Ux.

38. As noted in *The Wall Street Journal*, "[t]rade in personal data has emerged as a driver of the digital economy. Many tech companies offer products for free and get income from online ads that are customized using data about customers. These companies compete for ads, in part, based on the quality of the information they possess about users." Angwin & Valentino-Devries, *Google's iPhone Tracking: Web Giant, Others Bypassed Apple Browser Settings for Guarding Privacy*.

39. Google Inc. ("Google") also acknowledges the value of web browsing histories by purchasing such histories directly from web users. Google's "Screenwise" panel is a program whereby a few thousand Google users are allowing Google to track their web browsing histories in return for up to $25 in gift cards. *See* http://www.google.com/landing/screenwisepanel/.

40. Defendant ultimately profited from using the information they collected after hacking Plaintiffs' and the Class members' Devices in, among other things, its online advertising business.

41. By the above actions, Defendant deprived Plaintiffs and the Class members of the ability to sell their personal information, including web browsing histories, to Defendant.

CLASS ACTION ALLEGATIONS

42. Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure 23 on behalf of a class of Internet users (collectively, the "Class") defined as follows:

> All Safari users (1) whose Privacy Controls were set to the Third-Party-Blocking Only Option, (2) who visited a web page containing a Hacking Ad that disabled their Privacy Controls with respect to Defendant, enabling Defendant to place the "VM_USR" cookie on the users' Devices, and (3) on whose Devices Defendant then placed the "VM_USR" cookie. The class period runs from the date that Defendant first began delivering Hacking Ads to web pages to the date of filing of this complaint (the "Class Period").

43. Plaintiffs also bring this action pursuant to Federal Rule of Civil Procedure 23 on behalf of a subclass of Internet users residing in New York (collectively, the "New York Subclass") defined as follows:

> All New York Safari users (1) whose Privacy Controls were set to the Third-Party-Blocking Only Option, (2) who visited a web page containing a Hacking Ad that disabled their Privacy Controls with respect to Defendant, enabling Defendant to place the "VM_USR" cookie on the users' Devices, and (3) on whose Devices Defendant then placed the "VM_USR" cookie; during the Class Period.

44. Plaintiffs also bring this action pursuant to Federal Rule of Civil Procedure 23 on behalf of a subclass of Internet users residing in California (collectively, the "California Subclass") defined as follows:

> All California Safari users (1) whose Privacy Controls were set to the Third-Party-Blocking Only Option, (2) who visited a web page containing a Hacking Ad that hacked their Privacy Controls, enabling Defendant to place the "VM_USR" cookie on the users' Devices, and (3) on whose Devices Defendant then placed the "VM_USR" cookie; during the Class Period.

45. Excluded from the Class are Defendant; any parent, subsidiary, or affiliate of Defendant or any employees, officers, or directors of Defendant; legal representatives, successors, or assigns of Defendant; and any justice, judge or magistrate judge of the United States who may hear the case, and all persons related to any such judicial officer, as defined in 28 U.S.C. § 455(b).

46. **Numerosity**. The Class members are so numerous and dispersed nationwide that joinder of all members is impracticable. Upon information and belief, there are millions of Internet users whose Safari Privacy Controls have been debilitated by Defendant's Hacking Ads. The exact number of Class members is unknown, but Plaintiffs reasonably estimate and believe that there are millions of persons in the Class.

47. **Commonality**. There are numerous and substantial questions of law and fact that are common to all members of the Class, which predominate over any question affecting only individual Class members. The members of the Class were and potentially continue to be subjected to the same practices of Defendant. The common questions and issues raised by Plaintiffs' claims include, *inter alia*, the following:

(a) whether Defendant hacked Plaintiffs' and the Class members' Devices using Hacking Ads; and

(b) whether Defendant collected Plaintiffs and the Class members' web browsing histories against their will.

48. **Typicality**. Plaintiffs' claims are typical of the claims of all of the other members of the Class, because their claims are based on the same legal and remedial theories as the claims of the Class and arise from the same course of conduct by Defendant.

49. **Adequacy**. Plaintiffs will fairly and adequately protect the interests of all members of the Class in the prosecution of this action and in the administration of all matters relating to the claims stated herein. Plaintiffs are similarly situated with, and have suffered similar injuries to, the members of the Class they seek to represent. Plaintiffs have retained counsel experienced in handling class action lawsuits. Neither Plaintiffs nor their counsel have any interest that might cause them not to vigorously pursue this action.

50. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of the controversy, since individual joinder of the Class members is impracticable. Even if individual Class members were able to afford individual litigation, it would be unduly burdensome to the Courts in which the individual litigation would proceed. Defendant has subjected the Class to the same violations as referenced herein. Accordingly, class certification is appropriate under Rule 23 because common issues of law and fact regarding Defendant's uniform violations predominate over individual issues, and class certification is a superior method of resolving these claims. No unusual difficulties are likely to be encountered in the management of this action as a class action. Defendant has acted in a manner that affects Plaintiffs and all Class members alike, thereby making appropriate injunctive, declaratory, and other relief appropriate with respect to the Class as a whole.

CAUSES OFACTION

COUNT ONE

(VIOLATION OF NEW YORK GENERAL BUSINESS LAW § 349)

51. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.

52. New York General Business Law § 349 prohibits "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state…."

53. In violation of § 349, Defendant engaged in material, deceptive, consumer-oriented acts in the conduct of business that injured Plaintiffs and the Class members.

54. Specifically, Plaintiffs and the Class members mistakenly believed that viewing web pages that included Hacking Ads would not harm their Devices.

55. Defendant's Hacking Ads appeared to be a non-invasive, benign part of the digital environment.

56. In reality, Defendant used its Hacking Ads to harm Plaintiffs' and the Class members' Devices by debilitating the functionality of their Safari Privacy Controls, as described herein.

57. Further, Plaintiffs and the Class members mistakenly believed that Defendant would respect that they, via Safari's Privacy Controls, had explicitly denied permission to Defendant to use Third Party Content in conjunction with cookies to obtain End User Information about them.

58. In reality, Defendant ignored Plaintiffs' and the Class members' explicit prohibition, disabled the functionality of Safari's Privacy Controls, and used its Third Party Content in conjunction with cookies it set on Plaintiffs' and the Class members' Devices to obtain End User Information about Plaintiffs and the Class members as they visited web pages throughout the web.

59. Defendant's acts and/or omissions were generally aimed at the consuming public.

60. These unlawful deceptive acts directly and proximately caused harm to Plaintiffs and the Class members in the following ways:

(a) through the degradation in value of their Devices;

(b) through the loss of their privacy and the exposure of their personal, sensitive, and private information, as a result of which Plaintiffs and the Class members were shocked, humiliated, and angered and suffered emotional distress;

(c) by depriving Plaintiffs and the Class members of the ability to sell their personal information, including *their web browsing histories*, *to* Defendant.

61. As a direct and proximate result of Defendant's violation of § 349, Plaintiffs and the Class members have suffered damages in an amount to be determined at trial.

62. Plaintiffs and the Class members have also suffered irreparable injury as a result of Defendant's unlawful conduct, including the unauthorized collection of their personal information. Additionally, because the stolen information cannot be returned, the harm from the security breach is ongoing and compounding. Accordingly, Plaintiffs and the Class members have no adequate remedy at law, entitling them to injunctive relief.

COUNT TWO

(VIOLATION OF THE CALIFORNIA COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT, CALIFORNIA PENAL CODE § 502)

63. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.

64. California Penal Code § 502(c)(1) prohibits a person from knowingly accessing and without permission altering, damaging, and/or otherwise using data, computers, computer systems, and/or computer networks to:

(A) execute a scheme or artifice to defraud or deceive, and/or

(B) wrongfully control or obtain money, property, or data.

65. In violation of § 502(c)(1), Defendant intentionally and without permission altered, damaged, and otherwise used Plaintiffs' and the Class members' Devices to execute a scheme or artifice to defraud or deceive.

66. Specifically, as described in detail herein, Defendant hacked Plaintiffs' and the Class members' Devices as part of the execution of a scheme in which Defendant intentionally failed to inform Plaintiffs and the Class members that Defendant had hacked their Devices and

subsequently used Third Party Content in conjunction with cookies to End User Information about Plaintiffs and the Class members as they surfed the web.

67. In violation of § 502(c)(1), Defendant intentionally and without permission altered, damaged, and otherwise used Plaintiffs' and the Class members' Devices to wrongfully control or obtain money, property, or data.

68. Specifically, as described in detail herein, Defendant hacked Plaintiffs' and the Class members' Devices without their knowledge to obtain personal data about them, including their web browsing histories. Further, the personal data that Defendant obtained is property.

69. California Penal Code § 502(c)(2) prohibits a person from knowingly accessing and without permission taking, copying, and/or making use of data from a computer, computer system, and/or computer network.

70. In violation of § 502(c)(2), Defendant intentionally and without permission took, copied, and/or made use of data from Plaintiffs' and the Class members' Devices.

71. Specifically, as described in detail herein, Defendant hacked Plaintiffs' and the Class members' Devices and took information about their web surfing from the Devices, which Defendant made use of in its advertising business.

72. California Penal Code § 502(c)(3) prohibits a person from knowingly and without permission using "computer services" as that term is defined in California Penal Code § 502(b)(4).

73. In violation of § 502(c)(3), Defendant intentionally and without permission used "computer services," including but not limited to storage functions and web history tracking.

74. Specifically, as described in detail herein, Defendant hacked Plaintiffs' and the Class members' Devices, stored cookies on the Devices, and used those cookies in conjunction with browser software on the Devices to obtain End User Information about Plaintiffs and the Class members as they browsed web pages to which Defendant delivered Third Party Content.

75. California Penal Code § 502(c)(4) prohibits a person from knowingly and without permission adding, altering, and/or damaging data, computer software, and/or computer

programs that reside and/or exist internal and/or external to a computer, computer system, and/or computer network.

76. In violation of § 502(c)(4), Defendant intentionally and without permission added, altered, and/or damaged data, computer software, and/or computer programs that resided internal to Plaintiffs' and the Class members' Devices.

77. Specifically, as described in detail herein, Defendant hacked Plaintiffs' and the Class members' Safari Privacy Controls, debilitating their functionality.

78. Further, Defendant intentionally and without permission added cookies to Plaintiffs' and the Class members' Devices.

79. California Penal Code § 502(c)(5) prohibits a person from knowingly and without permission disrupting and/or causing the disruption of "computer services" (as that term is defined in California Penal Code § 502(b)(4)) to an authorized user of a computer, computer system, and/or computer network.

80. In violation of § 502(c)(5), as described in detail herein, Defendant disabled the functionality of Plaintiffs' and the Class members' Safari Privacy Controls, thereby disrupting Plaintiffs' and the Class members' desired use of their web browsers and the World Wide Web.

81. California Penal Code § 502(c)(7) prohibits a person from knowingly and without permission accessing computers, computer systems, and/or computer networks.

82. In violation of § 502(c)(7), as described in detail herein, Defendant hacked Plaintiffs' and the Class members' Safari Privacy Controls and placed cookies on their Devices, which Defendant used in conjunction with Third Party Content to obtain End User Information about them as they surfed the web.

83. California Penal Code § 502(c)(8) prohibits a person from knowingly introducing "computer contaminants" – as defined in California Penal Code § 502(b)(10) – into computers, computer systems, and/or computer networks.

84. In violation of § 502(c)(8), as described in detail herein, Defendant intentionally introduced computer programming code into Plaintiffs' and the Class members' Devices that

"usurp[ed] the normal operation" of the Devices by hacking Safari's Privacy Controls, enabling the placement of cookies on the Devices.

85. As a direct and proximate result of Defendant's violation of California Penal Code § 502, Defendant caused loss to Plaintiffs and the Class members in an amount to be proven at trial.

86. Plaintiffs and the Class members are entitled to recovery of attorneys' fees pursuant to § 502(e).

87. Plaintiffs and the Class members are entitled to punitive or exemplary damages under California Penal Code § 502(e)(4) because Defendant willfully violated § 502(c) and is guilty of "fraud" as defined by California Civil Code § 3294(c)(3).

88. Under § 3294(c)(3), "fraud" means an intentional misrepresentation, deceit, or concealment of a material fact known to the defendant with the intention on the part of the defendant of thereby depriving a person of property or legal rights or otherwise causing injury.

89. As described in detail herein, Defendant intentionally concealed from Plaintiffs and the Class members the fact that Defendant dismantled the privacy safeguards established by their Privacy Controls.

90. As a result of concealing this fact, Defendant intended to and did deprive Plaintiffs and the Class members of their legal right to privacy.

91. Further, as a result of concealing this fact, Defendant intended to profit and did profit by obtaining without authorization personal, private, and sensitive information about Plaintiffs and the Class members as they surfed the web and using the information in connection with Defendant's advertising business. Defendant's actions deprived Plaintiffs and the Class of the opportunity to sell the information to Defendant. Defendant thereby deprived Plaintiffs and the Class members of valuable property.

92. Plaintiffs and the Class members have also suffered irreparable injury as a result of Defendant's unlawful conduct, including the unauthorized collection of their personal information. Additionally, because the stolen information cannot be returned, the harm from the

security breach is ongoing and compounding. Accordingly, Plaintiffs and the Class members have no adequate remedy at law, entitling them to injunctive relief.

COUNT THREE

<u>(VIOLATION OF ARTICLE I, SECTION 1 OF THE CALIFORNIA CONSTITUTION)</u>

93. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.

94. Article I, Section 1 of the California Constitution states that "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Cal. Const. art. I, § 1.

95. Plaintiffs and the Class members have a legally protected autonomy privacy interest in making intimate personal decisions regarding the use of their Devices without interference. This interest includes an interest in maintaining the integrity of their web browser privacy controls.

96. Plaintiffs and the Class members have a legally protected privacy interest in the End User Information (including personal, confidential, and sensitive information and web browsing histories) that Defendant obtained by hacking Plaintiffs' and the Class members' Safari Privacy Controls.

97. Plaintiffs and the Class members reasonably expected that they would be able to make intimate personal decisions regarding the use of their Devices free of interference, including decisions related to web browser privacy controls.

98. Plaintiffs and the Class members reasonably expected that their End User Information (including personal, confidential, and sensitive information) and intimate personal decisions would be kept private.

99. Defendant committed a serious invasion of Plaintiffs' and the Class members' privacy interests by hacking their Safari Privacy Controls. Unbeknownst to Plaintiffs and Class

members, Defendant made a private decision on behalf of Plaintiffs and the Class members that Defendant was not authorized to make.

100. Defendant committed a serious invasion of Plaintiffs' and the Class members' privacy interests by, after hacking their Safari Privacy Controls, obtaining End User Information (including personal, confidential, and sensitive information) about them as they surfed the web without authorization.

101. By the acts, transactions, and courses of conduct alleged herein, Defendant violated Plaintiffs' and the Class members' inalienable right to privacy.

102. As a consequence, Plaintiffs and the Class members were personally injured and suffered emotional distress damages.

COUNT FOUR

(VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT, CALIFORNIA PENAL CODE § 630 *ET SEQ.*)

103. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.

104. In violation of California Penal Code § 631, Defendant, by means of a contrivance (or in "any other manner") made an unauthorized connection, electrically or "otherwise", with the wires, lines, cables, or instruments within the State of California over which communications or messages traveled between Plaintiffs' and the Class members' web browsers and the websites whose web pages they visited.

105. Specifically, as described in detail herein, Defendant hacked Plaintiffs' and the Class members' Safari Privacy Controls, which enabled it to place cookies on Plaintiffs' and the Class members' devices that it was explicitly not authorized to place. The cookies so placed, when used in conjunction with delivery of Third Party Content to Plaintiffs and the Class members (as described above), enabled Defendant to obtain End User Information about Plaintiffs and the Class members that Defendant would not otherwise have been able to obtain. Accordingly, Defendant created an unauthorized connection to Plaintiffs' and the Class

members' communications with the websites whose web pages they visited, which occurred over wires, lines, cables, or instruments within the State of California.

106. In violation of California Penal Code § 631, Defendant willfully, intentionally, without the consent of Plaintiffs and the Class members, and in an unauthorized manner, obtained, read, attempted to read, learned, and/or attempted to learn the contents of Plaintiffs' and the Class members' electronic communications with (or messages to) the websites whose web pages they visited while the communications (or messages) were in transit in or through California and/or while they were being sent from or received at a place within California.

107. Further, websites whose web pages were visited by Plaintiffs and the Class members did not have the authority to consent to alteration by Defendant of Plaintiffs' and the Class members' Safari Privacy Controls.

108. Defendant used and communicated such illegally obtained electronic communications of Plaintiffs and the Class members, including use and communication in its online advertising business.

109. As a direct and proximate result of the above-described conduct by Defendant, Plaintiffs and all Class members have suffered, and, unless such conduct is enjoined, will continue to suffer, damages in an amount to be proven at trial.

110. Pursuant to California Penal Code § 637.2, Plaintiffs and the Class members are entitled to recover three times their actual and/or statutory damages from Defendant, for the conduct described herein.

111. Defendant's conduct is causing, and unless enjoined will continue to cause, Plaintiffs and the Class members great and irreparable injury that cannot be fully compensated for or measured in money. Plaintiffs and the Class members have no adequate remedy at law and, pursuant to California Penal Code § 637.2(b), are entitled to preliminary and permanent injunctions prohibiting further use and communication of their unlawfully obtained information.

COUNT FIVE

(TRESPASS TO PERSONAL PROPERTY / CHATTELS)

112. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.

113. The common law of New York prohibits the intentional intermeddling with personal property in possession of another that results in the deprivation of the use of the personal property or impairment of the condition, quality, or usefulness of the personal property.

114. In violation of New York common law and as detailed more fully herein, Defendant dispossessed Plaintiffs and the Class members from use and/or access to their Devices, or parts of them, without their knowledge or consent. Further, Defendant's acts constituted an intentional interference with the use and enjoyment of the Devices.

115. Without Plaintiffs' and the Class members' knowledge or consent, Defendant knowingly and intentionally accessed their property and caused them injury.

116. Defendant engaged in deception and concealment in order to gain access to Plaintiffs' and the Class members' Devices.

117. Defendant's hacking of Safari's Privacy Controls and subsequent installation of cookies on Plaintiffs' and the Class members' Devices interfered and/or intermeddled with the Devices, including by altering or damaging controls designed to prevent the information collection effected by Defendant. Such use, interference, and/or intermeddling was without the knowledge or consent of Plaintiffs and the Class members.

118. Defendant's hacking of Plaintiffs' and the Class members' Devices and subsequent placement of cookies on them impaired their condition and value. In particular, these actions debilitated the functionality of Plaintiffs' and the Class members' Safari Privacy Controls.

119. Defendant's trespass to chattels, nuisance, and interference caused real and substantial damage to Plaintiffs and the Class members.

120. As a direct and proximate result of Defendant's trespass to chattels, nuisance, interference, and unauthorized access to and intermeddling with Plaintiffs' and the Class members' Devices, Defendant has injured and impaired the condition and value of the Devices as follows:

(a) By consuming the resources of and/or degrading the performance of Plaintiffs' and the Class members' Devices (including space, memory, processing cycles, and Internet connectivity);

(b) By diminishing the use of, value, speed, capacity, and/or capability of Plaintiffs' and the Class members' Devices;

(c) By altering and controlling the functioning of Plaintiffs' and the Class members' Devices;

(d) By devaluing, interfering with, and/or diminishing Plaintiffs' and the Class members' possessory interest in their Devices;

(e) By infringing on Plaintiffs' and the Class members' right to exclude others from their Devices;

(f) By infringing on Plaintiffs' and the Class members' right to determine, as owners of their Devices, which programs should be installed and operated on the Devices, and how programs should be installed and operated on the Devices;

(g) By compromising the integrity, security, and ownership of Plaintiffs' and the Class members' Devices;

(h) By forcing Plaintiffs and the Class members to expend time and resources in order to remove the cookies installed on their Devices without notice or consent.

121. Plaintiffs and the Class members have no adequate remedy at law.

COUNT SIX

(INVASION OF PRIVACY IN VIOLATION OF CALIFORNIA COMMON LAW)

122. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.

123. Defendant intruded on Plaintiffs' and the Class members' private affairs and seclusion by hacking their Safari Privacy Controls and placing cookies on their Devices – conduct that Defendant engaged in completely outside of their knowledge and against their express will. The cookies enabled Defendant, without authorization, to obtain End User Information about Plaintiffs and the Class members as they surfed the web, as more fully detailed herein.

124. Plaintiffs and the Class members have a legally protected autonomy privacy interest in making intimate personal decisions regarding the use of their Devices without interference. This interest includes an interest in maintaining the integrity of their web browser privacy controls.

125. Plaintiffs and the Class members have a legally protected privacy interest in the End User Information (including personal, confidential, and sensitive information and web browsing histories) that Defendant obtained by hacking Plaintiffs' and the Class members' Safari Privacy Controls.

126. Plaintiffs and the Class members reasonably expected that they would be able to make intimate personal decisions regarding the use of their Devices free of interference, including decisions related to web browser privacy controls.

127. Plaintiffs and the Class members reasonably expected that their End User Information (including personal, confidential, and sensitive information) and intimate personal decisions would be kept private.

128. Defendant intentionally committed a "serious invasion of privacy" that would be highly offensive to a reasonable person by hacking Plaintiffs' and the Class members' Safari Privacy Controls. Unbeknownst to Plaintiffs and the Class members, Defendant made a private

decision on behalf of Plaintiffs and the Class members that Defendant was not authorized to make.

129. Defendant intentionally committed a "serious invasion of privacy" that would be highly offensive to a reasonable person by, after hacking Plaintiffs' and the Class members' Safari Privacy Controls, obtaining End User Information about them as they surfed the web without authorization.

130. As a consequence, Plaintiffs and the Class members were personally injured and suffered emotional distress damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and members of the Class seek relief against Defendant as follows:

A. An order certifying that this action is properly brought and may be maintained as a class action under Rule 23 of the Federal Rules of Civil Procedure, that Plaintiffs be appointed as Class Representatives, and that Plaintiffs' counsel be appointed Class Counsel.

B. Awarding damages as alleged above.

C. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class members, including, *inter alia*, an order prohibiting Defendant from engaging in the wrongful and unlawful acts described herein.

D. Disgorgement of all revenue earned from selling or otherwise using or trading on the private information obtained from Plaintiffs and the Class members as a result of hacking their Devices, as described herein.

E. Awarding Plaintiffs and the Class members their reasonable litigation expenses and attorneys' fees; and

F. Awarding such other and further relief at law or equity as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs and the Class members hereby demand trial of their claims by jury to the extent authorized by law.

DATED: May 25, 2012

REESE RICHMAN LLP

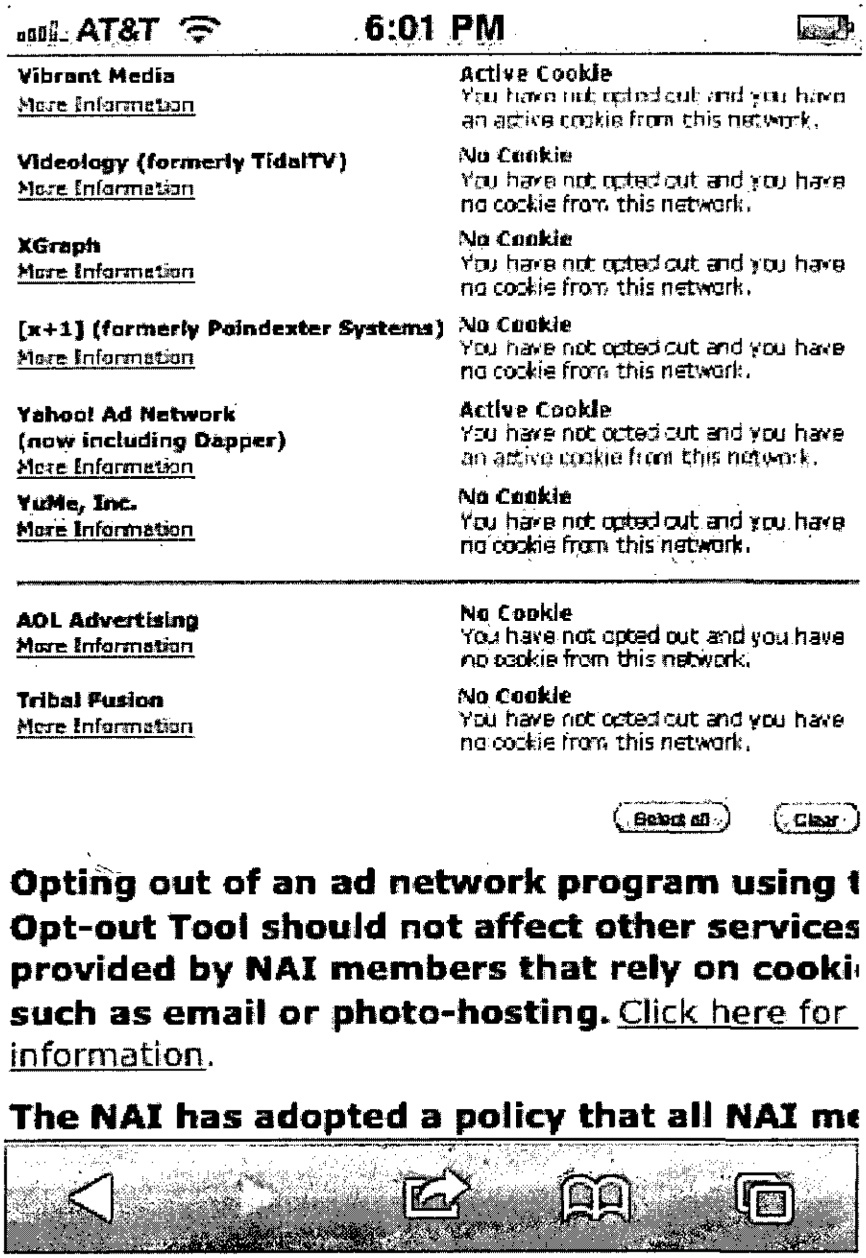
Kim E. Richman
krichman@reeserichman.com
Michael R. Reese
mreese@reeserichman.com
875 Avenue of the Americas, 18th Floor
New York, New York 10001
Telephone: (212) 643-0500
Facsimile: (212) 253-4272

– and –

MILBERG LLP
Sanford P. Dumain
sdumain@milberg.com
Peter Seidman
pseidman@milberg.com
One Penn Plaza
New York, New York 10119
Telephone: (212) 594-5300
Facsimile: (212) 868-1229

Attorneys for Plaintiffs and the Proposed Class

EXHIBIT 1



Vibrant Media More Information	**Active Cookie** You have not opted out and you have an active cookie from this network.
Videology (formerly TidalTV) More Information	**No Cookie** You have not opted out and you have no cookie from this network.
XGraph More Information	**No Cookie** You have not opted out and you have no cookie from this network.
[x+1] (formerly Poindexter Systems) More Information	**No Cookie** You have not opted out and you have no cookie from this network.
Yahoo! Ad Network (now including Dapper) More Information	**Active Cookie** You have not opted out and you have an active cookie from this network.
YuMe, Inc. More Information	**No Cookie** You have not opted out and you have no cookie from this network.
AOL Advertising More Information	**No Cookie** You have not opted out and you have no cookie from this network.
Tribal Fusion More Information	**No Cookie** You have not opted out and you have no cookie from this network.

Opting out of an ad network program using t Opt-out Tool should not affect other services provided by NAI members that rely on cooki such as email or photo-hosting. Click here for information.

The NAI has adopted a policy that all NAI me